[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Wintersemester 2021, Mittwoch, 24.02.2021, 14:00 Uhr

Name:_____ Punkte:_____/100 (40 zum Bestehen) Note:____

Disclaimer:
- Zugelassene Hilfsmittel: keine ausser Stifte und Lineal
- Der Lösungsweg muss bei allen Aufgaben ersichtlich sein

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Ihr Unternehmen SpaceY möchte eine Menge „Cloudlink“ genannte Satelliten in die Erdumlaufbahn schicken.

Dabei ist natürlich auch die Cybersecurity ein zentrales Thema. Schreiben Sie für Ihren Hauptinverstor Anton Mask zunächst ein Glossar mit kurzen Erklärungen für die folgenden Begriffe aus dem Themenbereich:

Zero-Trust, Buffer Overflow, USV, Schutzziele, Proxy, Threat Model, OWASP Top10, Virus, ISO 27001, Shell Code

Aufgabe 2: Safety

A)__/8 B)__/8 C)__/6 D)__/8 __/30 Punkte

A) Beim Satellitennetzwerk ist natürlich die Kommunikationsinfrastruktur eine kritische Komponente. Jeder Satellit besitzt dazu 2 Kommunikationsmodule die jeweils eine Verfügbarkeit von 80% aufweisen. Die Antenne ist mit einer Verfügbarkeit von 99% angegeben und deshalb nur ein Mal vorhanden. Zudem ist natürlich die Energieversorgung entscheidend die durch ein Solarmodul – 60% Verfügbarkeit oder alternativ über eine Batterie (90% Verfügbarkeit) ausgelegt sind.
Wie viele Stunden im Jahr ist ein Satellit statistisch gesehen nicht erreichbar?

B) Wenn ein drittes Kommunikationsmodul eingebaut würde – wie würde sich die statistische Erreichbarkeit für ein Jahr verändern?

C) Ihr Investor plant auch eine bemannte Mission zum Mars. Sie sind beauftragt die Anforderungen für die Triebwerkssteuerung zu schreiben – würden Sie hier eher Verfügbarkeit oder Zuverlässigkeit fordern? Begründen Sie Ihre Anforderung. Welche Art von Redundanz würden Sie hier einsetzen?

D) Die Zuordnung zu verschiedenen Maßnahmen-Klassen ist im Lastenheft wohl auch noch nicht ausgefüllt worden. Bitte helfen Sie, indem Sie die Maßnahmen den Schutzzielen in der unten stehenden Tabelle zuordnen:

	Redundanz	**„Firewall++“**	**Kryptographie**	**Policies**
Verfügbarkeit				
Integrität				
Vertraulichkeit				
Zurechenbarkeit				
Rechtsverbindlichkeit				

Aufgabe 3: Security

A)__/5 B)__/5 C)__/5 D)__/5 E)__/5 F)__/7 G)__/6 H)__/9 I)__/8 J)__/5 __/60 Punkte

A) Software, die für das Satelitennetzwerk notwendig ist, entsteht in einem Entwicklungsprozess den man in verschiede Phasen unterteilen kann. Ordnen sie die SSDLC Aktivitäten der richtigen Phase zu:

Anforderungsphase	Fuzzing Tests
Entwurfsphase	Bedrohungsmodellierung
Entwicklungsphase	Reaktionsplan
Überprüfungsphase	Risikobewertung
Deploymentphase	Statische Code Analyse

B) Sie hatten als Penetrationtester die Aufgabe die Sicherheit des Cloudlink Satelitennetzwerkes zu testen. Es ist Ihnen gelungen einen Bot zu schreiben, der mit Hilfe eines Buffer Overflows alle Satelliten befällt. Skizzieren Sie zur Verdeutlichung der Funktionsweise in Pseudocode diesen Bot.

C) Bei der Ausnutzung solcher Buffer Overflows werden oft NOP-Rutschen verwendet. Zu welchem Zweck? Wie lange sollte so eine NOP-Rutsche sein?

D) Neben technischen Maßnahmen sind auch Regeln ein wichtiger Mechanismus, um Security zu stärken. Entwerfen Sie eine Policy (min. 5 Regeln) für Admins, die Wartungsarbeiten Vor Ort im RZ von SpaceY vornahmen müssen.

E) Identitäten spielen bei der Sicherheit eine große Rolle. Welche Identitäten auf welchen Ebenen könnte ein Satellit haben? Nennen Sie 3 Möglichkeiten diese zu Spoofen und beschreiben Sie im Sinne eines Threat Modells welche Maßnahmen Sie empfehlen würden um diese Angriffe zu verhindern.

E) Welche der folgenden Aussagen sind falsch (bitte streichen):

- Stateful Insprection Filter funktionieren nur mit zustandsbehafteten Protokollen
- Statische Filter arbeiten mit Heuristiken
- Beim Erstellen von Filterregeln sollten nur ungewünschte Vorgänge gefiltert werden
- Intrusion Prevention Systeme finden alle Attacken
- Intrusion Prevention Systeme müssen nur einmalig konfiguriert werden
- Statische Filter schreibt man am besten selbst
- Dynamische Filter können per Rate Limit implementiert sein
- Statische Filter lassen sich durch Spoofing täuschen

F) Welche der folgenden Strategien dienen insbesondere zum Denial of Service ?

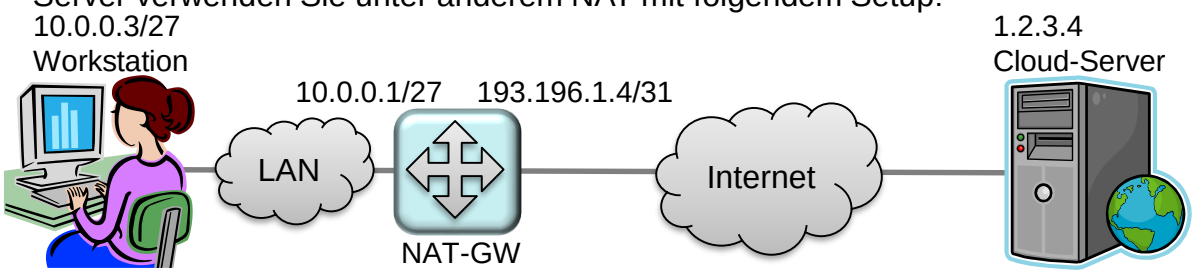
[ ] Ausnützen von Protokollschwächen
[ ] Social Engineering
[ ] Überladen von Diensten
[ ] Lambda 8300
[ ] Ausnützen von Programmierfehlern
[ ] Cross Site Request Forgery

G) SpaceY ist in letzter Zeit Ziel einiger DDoS Attacke geworden.
Wie können Sie Ihr Unternehmen davor schützen?

H) Was kann ein Circuit Level Proxy leisten? Kreuzen Sie an

[ ] Über Routing-Grenzen hinweg Verbindungen aufbauen
[ ] Die Bandbreite verdoppeln
[ ] Client und Server des Application Level Protokolls implementieren
[ ] Social Engineering

I) Bei der Anbindung der Arbeitsplätze in Ihrer Raumfahrtzentrale an Ihre Cloud-Server verwenden Sie unter anderem NAT mit folgendem Setup:



Die Workstation soll zum Cloud-server zwei HTTPS-Verbindungen aufmachen. Füllen Sie die folgende NAT-Tabelle des NAT-GW mit den dann vorzufindenden Inhalten:

SRC IP	SRC PORT	NAT IP	NAT PORT	DST IP	DST PORT